10/031065 (5610)

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GEM 736	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/02009	International filing date (*day month year*) 12 July 2000 (12.07.00)	Priority date (*day month year*) 15 July 1999 (15.07.99)
International Patent Classification (IPC) or national classification and IPC G06F 7/58		
Applicant GEMPLUS		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
13 February 2001 (13.02.01)	29 March 2001 (29.03.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR00/02009

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1-7 . as originally filed
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

☒ the claims:

pages 1-8 . as originally filed
pages _____ . as amended (together with any statement under Article 19
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

☐ the drawings:

pages _____ . as originally filed
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

☐ the sequence listing part of the description:

pages _____ . as originally filed
pages _____ . filed with the demand
pages _____ . filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-8	YES
	Claims		NO
Inventive step (IS)	Claims	1-8	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-8	YES
	Claims		NO

2. Citations and explanations

1. The invention relates to an improvement to a method for generating random numbers used in cryptosystems such as smart card random number generators.

2. The ANSI X9.17 standard specifies a method for generating a random number on the basis of a function having an inverse that is difficult to compute.

It has become apparent that the implementation of a secret key encryption algorithm (for example the DES algorithm) in a smart card is vulnerable to attacks whereby the secret key is discovered by means of a differential power analysis. The principle of these DPA attacks is based on the fact that the power consumption of the microprocessor executing instructions varies depending on the data handled. In order to find the secret key, the input or output message of the encryption algorithm must be known.

It follows that the two random number generation methods described in the introductory part of the application are vulnerable to DPA attacks because the random numbers output by these two methods are

the output messages of the encryption algorithm.

On the basis the power consumption of the smart card, it is therefore possible to discover the encryption key k and, thereafter, to predict the output of the random generator.

3. The method of the invention consists of modifying the random number generation methods described above in such a way that they are resistant to attacks such as DPA attacks. Said two methods are modified in that an intermediate integer variable is inserted into the computing loop just after S has been replaced with S xor I, which variable will adopt the value of the result of the encryption of S with the DES algorithm using the key K.

In this improved random number generation method, an attack involving the measurement of power, such as a DPA attack, is impossible because the input and output messages of the DES encryption algorithm are not known.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. In the claims, only reference signs referring to the drawing(s) should be placed between parentheses. The expression "for Data Encryption Standard" should not be placed between parentheses (PCT Article 6) because it defines the acronym DES.

2. The expressions "the quality of which is deemed to be inadequate" and "of inadequate quality" in Claim 2 are vague and ambiguous and cast doubt on the meaning of the technical features to which they refer. It follows that the subject matter of said claim is not clearly defined (PCT Article 6). Furthermore, the application does not contain any information defining this criterion of quality.

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
25 janvier 2001 (25.01.2001)

PCT

(10) Numéro de publication internationale
WO 01/06350 A1

(51) Classification internationale des brevets[7]: G06F 7/58

(21) Numéro de la demande internationale:
PCT/FR00/02009

(22) Date de dépôt international: 12 juillet 2000 (12.07.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:
99/09316 15 juillet 1999 (15.07.1999) FR

(71) Déposant *(pour tous les États désignés sauf US)*: GEMPLUS [FR/FR]; Parc d'activités de Gemenos, Avenue du Pic de Bertagne, F-13881 Gemenos (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)*: CORON, Jean-Sébastien [FR/FR]; 4, rue Léon de Lagrange, F-75015 Paris (FR). NACCACHE, David [FR/FR]; 7, rue Chaptal, F-75009 Paris (FR).

(74) Mandataire: BRUYERE, Pierre; Gemplus, Parc d'activités des Gemenos, Avenue du Pic de Bertagne, F-13881 Gemenos (FR).

(81) États désignés *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)*: brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée:
— *Avec rapport de recherche internationale.*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: METHOD FOR IMPROVING A RANDOM NUMBER GENERATOR TO MAKE IT MORE RESISTANT AGAINST ATTACKS BY CURRENT MEASURING

(54) Titre: PROCEDE D'AMELIORATION D'UN GENERATEUR ALEATOIRE EN VUE DE LE RENDRE RESISTANT CONTRE LES ATTAQUES PAR MESURE DE COURANT

(57) Abstract: The invention concerns a modification of two methods for random number generation to make them more resistant to attacks by current measuring. It is particularly designed to be implemented in electronic devices such as smart cards, PCMCIA, badges, contactless cards or any other portable device. It consists in: encrypting with the DES algorithm using the key K a value D representing a date information and introducing the result in an integer variable I; 2) for j ranging from 1 to m: 2a) substituting s with s x or I; 2b) introducing in the integer variable y the result of the encryption of s with the DES algorithm using the key K; 2c) introducing in xj the result of y or s; 2d) substituting s with y x or I; 2e) introducing in s the result of the encryption of s with the DES algorithm using the key K; 3) restoring in output the sequence (x1, x2, , xm).

(57) Abrégé: La présente invention concerne une modification de deux procédés de génération de nombre aléatoire en vue de les rendre résistants contre des attaques par mesure de courant. Elle est particulièrement destinée à être mise en oeuvre dans des dispositifs électroniques du type carte à puce, PCMCIA, badges, cartes sans contact ou tout autre appareil portable. 1) Chiffrer avec l'algorithme DES utilisant la clef K une valeur D représentant une information de date et mettre le résultat dans une variable entière I; 2) pour j allant de 1 à m faire: 2a) remplacer s par s xor I; 2b) mettre dans la variable entière y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K; 2c) mettre dans xj le résultat de y xor s; 2d) remplacer s par y xor I; 2e) mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K; 3) retourner en sortie la suite (x1, x2, ..., xm)

WO 01/06350 A1

PROCEDE D'AMELIORATION D'UN GENERATEUR ALEATOIRE EN VUE DE LE RENDRE RESISTANT CONTRE LES ATTAQUES PAR MESURE DE COURANT

L'invention concerne une amélioration d'un procédé de génération de nombres aléatoires ou source aléatoire, en particulier des sources mises au point dans le cadre de systèmes cryptographiques tels que les générateurs de nombres aléatoires embarqués à bord de cartes à puce.

Elle est particulièrement destinée à être mise en oeuvre dans le test et la validation de dispositifs électroniques du type carte à puce, PCMCIA, badges, cartes sans contact ou tout autre appareil portable.

La plupart des systèmes de cryptographie à clé publique (dite aussi cryptographie asymétrique) et clé secrète (dite aussi cryptographie symétrique) nécessitent le tirage d'aléas secrets. Il est primordial que de tels aléas, ou nombres, destinés à servir comme clés ultérieurement , soient à priori imprévisibles et ne présentent pas de régularités permettant de les retrouver par des stratégies de recherche exhaustive ou exhaustive améliorée pour laquelle les clés les plus probables sont cherchées en premier lieu.

Il est possible de construire une source aléatoire à partir d'une fonction dont il est difficile de calculer l'inverse. Soit f une

telle fonction. Il est possible de construire une source aléatoire en commençant par sélectionner une variable d'initialisation aléatoire s et en appliquant la fonction f à la suite de valeurs s, s+1, s+2,…La sortie de la source aléatoire est définie comme f(s),f(s+1),f(s+2),…En fonction des propriétés de la fonction f utilisée, il peut être préférable de ne garder que quelques bits de la sortie f(s),f(s+1),f(s+2)…

Une méthode de génération de nombre aléatoire à partir d'une fonction dont il est difficile de calculer l'inverse est spécifiée dans le standard ANSI X9.17. La méthode utilise l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, qui ne doit être utilisée que dans le cadre de cet algorithme. Le procédé de génération de nombre aléatoire prend en entrée un entier aléatoire et secret s de taille 64 bits et un entier m, et renvoie en sortie m entiers aléatoires de 64 bits x_1, x_2,…, x_m. Le procédé est caractérisé par les trois étapes suivantes :

1) Chiffrer avec l'algorithme DES utilisant la clef K une valeur D représentant une information de date et mettre le résultat dans la variable entière I.

2) Pour j allant de 1 à m exécuter les étapes suivantes :

2)a) Remplacer s par s xor I.

2)b) Mettre dans x_j le résultat du chiffrement de s avec l'algorithme DES utilisant la clef secrète K.

2)c) Remplacer s par x_j xor I.

2)d) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef secrète K.

3) Retourner en sortie la suite (x_1, x_2,…, x_m).

Il est possible d'utiliser ce générateur aléatoire dans une application pour laquelle un générateur aléatoire est déjà disponible, mais de qualité jugée insuffisante, par exemple un générateur aléatoire embarqué dans le microprocesseur d'une carte à puce. Dans ce cas, le procédé décrit précédemment est utilisé pour améliorer la qualité du générateur aléatoire. Ce procédé prend en entrée un entier aléatoire et secret s de taille 64 bits et un entier m, et renvoie en sortie m entiers aléatoires de 64 bits x_1, x_2,…, x_m. Le procédé utilise l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, qui ne doit être utilisée que dans le cadre de cet algorithme. Le procédé utilise une source S de qualité jugée insuffisante d'entiers aléatoires sur 64 bits. Le procédé est caractérisé par les 3 étapes suivantes :

1) Pour j allant de 1 à m faire

1)a) Générer un entier I à l'aide de la source S.

1)b) Remplacer s par s xor I.

1)c) Mettre dans x_j le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.

1)d) Générer un entier I à l'aide de la source S.

1)e) Remplacer s par x_j xor I.

1)f) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.

2) Retourner en sortie la suite (x_1, x_2,..., x_m).

Il est apparu que l'implémentation sur carte à puce d'un algorithme de chiffrement à clé secrète (par exemple l'algorithme DES) était vulnérable à des attaques consistant en une analyse différentielle de consommation de courant permettant de retrouver la clé secrète. Ces attaques sont appelées attaques DPA, acronyme pour Differential Power Analysis. Le principe de ces attaques DPA repose sur le fait que la consommation en courant du microprocesseur exécutant des instructions varie selon la donnée manipulée. Pour retrouver la clef secrète, il est nécessaire que le message d'entrée ou le message de sortie de l'algorithme de chiffrement soient connus.

Les deux procédés de génération de nombre aléatoire décrits précédemment sont donc vulnérables à des attaques de type attaques DPA. En effet, les nombres aléatoires renvoyés en

sortie par ces deux procédés sont les messages de sortie de l'algorithme de chiffrement. A partir de la consommation de courant de la carte à puce, il est donc possible de retrouver la clef K de chiffrement, et donc de prévoir ensuite la sortie du générateur aléatoire.

Le procédé de l'invention consiste en une modification des procédés de générations de nombre aléatoire décrits précédemment de façon à les rendre résistant contre des attaques de type DPA.

Le premier procédé modifié de générations de nombre aléatoire utilise l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, qui ne doit être utilisée que dans le cadre de cet algorithme. Il prend en entrée un entier aléatoire et secret s de taille 64 bits et un entier m, et renvoie en sortie m entiers aléatoires de 64 bits x_1, x_2,..., x_m. Le procédé utilise une variable entière intermédiaire y. Le procédé est caractérisé par les trois étapes suivantes :

1) Chiffrer avec l'algorithme DES utilisant la clef k une valeur D représentant une information de date et mettre le résultat dans la variable entière I.

2) Pour j allant de 1 à m exécuter les étapes suivantes :

2)a) Remplacer s par s xor I.

2)b) Mettre dans la variable entière y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.

2)c) Mettre dans x_j le résultat de y xor s.

2)d) Remplacer s par y xor I.

2)e) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.

3) Retourner en sortie la suite (x_1, x_2,…, x_m).

Dans ce procédé amélioré de génération de nombres aléatoires, une attaque par mesure de courant de type DPA est impossible car les messages d'entrée et de sortie de l'algorithme de chiffrement DES ne sont pas connus.

Le second procédé amélioré de génération de nombre aléatoire est utilisé pour augmenter la qualité d'un générateur aléatoire dont la qualité est jugée insuffisante. Ce procédé prend en entrée un entier aléatoire et secret s de taille 64 bits et un entier m, et renvoie en sortie m entiers aléatoires de 64 bits x_1, x_2,…, x_m. Le procédé utilise l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, qui ne doit être utilisée que dans le cadre de cet algorithme. Le procédé utilise une source S de qualité jugée insuffisante d'entiers aléatoires sur 64 bits. Le procédé est caractérisé par les deux étapes suivantes :

1) Pour j allant de 1 à m faire

1)a) Générer un entier I à l'aide de la source S.

1)b) Remplacer s par s xor I.

1)c) Mettre dans y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.

1)d) Mettre dans x_i le résultat de y xor s.

1)e) Remplacer s par y xor I.

1)f) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K.

3) Retourner en sortie la suite (x_1, x_2,…, x_m).

Dans ce procédé amélioré de génération de nombres aléatoires, une attaque par mesure de courant de type DPA est impossible car les messages d'entrée et de sortie de l'algorithme de chiffrement DES ne sont pas connus.

Les deux procédés de génération de nombre aléatoires précédemment décrits permettent donc d'obtenir un générateur de nombre aléatoire résistant contre les attaques par mesure de courant de type DPA.

REVENDICATIONS

1- Procédé de génération de nombre aléatoire utilisant l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, ladite clef K ne devant être utilisée que dans le cadre de cet algorithme, ledit procédé prenant en entrée un entier aléatoire et secret s de taille 64 bits et un paramètre entier m, ledit procédé renvoyant en sortie m entiers aléatoires de 64 bits x_1, x_2,…, x_m, caractérisé en ce qu'il comprend trois étapes :

1) Chiffrer avec l'algorithme DES utilisant la clef K une valeur D représentant une information de date et mettre le résultat dans une variable entière I ;

2) Pour j allant de 1 à m faire :

2)a) Remplacer s par s xor I ;

2)b) Mettre dans la variable entière y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K ;

2)c) Mettre dans x_j le résultat de y xor s;

2)d) Remplacer s par y xor I ;

2)e) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef k ;

3) Retourner en sortie la suite (x_1, x_2,…, x_m).

2- Procédé de génération de nombre aléatoire permettant d'améliorer la qualité d'un générateur aléatoire dont la qualité est jugée insuffisante, ledit procédé prenant en entrée un entier aléatoire et secret s de taille 64 bits

et un entier m, ledit procédé renvoyant en sortie m entiers aléatoires de taille 64 bits x_1, x_2,…, x_m, ledit procédé utilisant l'algorithme DES (pour Data Encryption Standard) avec une clé secrète K, qui ne doit être utilisée que dans le cadre de cet algorithme, ledit procédé utilisant une variable intermédiaire entière y, ledit procédé utilisant une source S de qualité jugée insuffisante d'entiers aléatoires sur 64 bits x_1, x_2,…, x_m,, caractérisé en ce qu'il comprend les deux étapes suivantes :

1) Pour j allant de 1 à m faire

1)a) Générer un entier I à l'aide de la source S ;

1)b) Remplacer s par s xor I ;

1)c) Mettre dans y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef k ;

1)d) Mettre dans x_i le résultat de y xor s ;

1)e) Remplacer s par y xor I ;

1)f) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K ;

2) Retourner en sortie la suite (x_1, x_2,…, x_m).

3- Dispositif électronique mettant en œuvre le procédé selon l'une quelconque des revendications 1 et 2 caractérisé en ce que le dispositif est un dispositif portable.

4- Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une carte à puce.

5- Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une carte sans contact.

6- Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une carte PCMCIA.

7- Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est un badge.

8- Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une montre intelligente.

INTERNATIONAL SEARCH REPORT

In ational Application No
PCT/FR 00/02009

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
COMPENDEX, INSPEC, IBM-TDB, EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 672 402 A (GEMPLUS CARD INT) 7 August 1992 (1992-08-07) figure 1 ---	1,2
A	"DEA-BASED PSEUDORANDOM NUMBER GENERATOR" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, vol. 35, no. 1B, 1 June 1992 (1992-06-01), pages 431-434, XP000309126 ISSN: 0018-8689 the whole document --- -/--	1,2

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 October 2000	25/10/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Verhoof, P

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	"INITIALIZATION PROCEDURE FOR DEA-BASED PSEUDORANDOM NUMBER GENERATOR" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, vol. 35, no. 1B, 1 June 1992 (1992-06-01), pages 351-353, XP000309094 ISSN: 0018-8689 the whole document ---	1,2
A	WO 97 20266 A (BELL COMMUNICATIONS RES) 5 June 1997 (1997-06-05) page 5; figure 1 ---	1,2
A	THE PGP ATTACK FAQ, PART 4, 'Online! 26 January 1997 (1997-01-26), XP002137510 Retrieved from the Internet: <URL:http://www.stack.nl/{galactus/remailers/attack-4.html> 'retrieved on 2000-05-08! the whole document -----	1,2

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ional Application No
PCT/FR 00/02009

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2672402 A	07-08-1992	NONE	
WO 9720266 A	05-06-1997	US 5727063 A	10-03-1998
		CA 2238545 A	05-06-1997
		EP 0864124 A	16-09-1998
		JP 2963929 B	18-10-1999
		JP 11500849 T	19-01-1999

RAPPORT DE RECHERCHE INTERNATIONALE

De ande internationale No
PCT/FR 00/02009

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F7/58

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
COMPENDEX, INSPEC, IBM-TDB, EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	FR 2 672 402 A (GEMPLUS CARD INT) 7 août 1992 (1992-08-07) figure 1 ---	1,2
A	"DEA-BASED PSEUDORANDOM NUMBER GENERATOR" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, vol. 35, no. 1B, 1 juin 1992 (1992-06-01), pages 431-434, XP000309126 ISSN: 0018-8689 le document en entier --- -/--	1,2

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
18 octobre 2000	25/10/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Verhoof, P

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	"INITIALIZATION PROCEDURE FOR DEA-BASED PSEUDORANDOM NUMBER GENERATOR" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, vol. 35, no. 1B, 1 juin 1992 (1992-06-01), pages 351-353, XP000309094 ISSN: 0018-8689 le document en entier	1,2
A	WO 97 20266 A (BELL COMMUNICATIONS RES) 5 juin 1997 (1997-06-05) page 5; figure 1	1,2
A	THE PGP ATTACK FAQ, PART 4, 'en ligne! 26 janvier 1997 (1997-01-26), XP002137510 Extrait de l'Internet: <URL:http://www.stack.nl/(galactus/remailers/attack-4.html> 'extrait le 2000-05-08! le document en entier	1,2

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 00/02009

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2672402 A	07-08-1992	AUCUN	
WO 9720266 A	05-06-1997	US 5727063 A	10-03-1998
		CA 2238545 A	05-06-1997
		EP 0864124 A	16-09-1998
		JP 2963929 B	18-10-1999
		JP 11500849 T	19-01-1999

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	POUR SUITE A DONNER voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
GEM 736		
Demande internationale n°	Date du dépôt international *(jour/mois/année)*	(Date de priorité (la plus ancienne) *(jour/mois/année)*
PCT/FR 00/ 02009	12/07/2000	15/07/1999
Déposant		
GEMPLUS		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 4 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

   [ ] le texte est approuvé tel qu'il a été remis par le déposant

   [X] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° –

   [ ] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [X] Aucune des figures n'est à publier.

Cadre III TEXTE DE L'ABREGE (suite du point 5 de la première feuille)

1) Chiffrer avec l'algorithme DES utilisant la clef K une valeur D représentant une information de date et mettre le résultat dans une variable entière I ;
2) Pour j allant de 1 à m faire :
2)a) Remplacer s par s xor I ;
2)b) Mettre dans la variable entière y le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K ;
2)c) Mettre dans xj le résultat de y xor s ;
2)d) Remplacer s par y xor I ;
2)e) Mettre dans s le résultat du chiffrement de s avec l'algorithme DES utilisant la clef K ;
3) Retourner en sortie la suite (x1, x2,...,xm).

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire GEM 736	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/02009	Date du dépot international *(jour/mois/année)* 12/07/2000	Date de priorité *(jour/mois/année)* 15/07/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G06F7/58		
Déposant GEMPLUS et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

I	☒	Base du rapport
II	☐	Priorité
III	☐	Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
IV	☐	Absence d'unité de l'invention
V	☒	Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
VI	☐	Certains documents cités
VII	☐	Irrégularités dans la demande internationale
VIII	☒	Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
13/02/2001	29.03.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Nussbaumer, C N° de téléphone +49 89 2399 2145

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/02009

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17).*) :

   Description, pages:

   1-7 version initiale

   Revendications, N°:

   1-8 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.
   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
   ☐ remis ultérieurement à l'administration, sous forme écrite.
   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :
   ☐ des revendications, n^{os} :
   ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-8
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-8
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-8
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. L'invention concerne une amélioration d'un procédé de génération de nombres aléatoires mises au point dans le cadre de systèmes cryptographiques tels que les générateurs de nombres aléatoires embarqués à bord de cartes à puce.

2. Une méthode de génération de nombre aléatoire à partir d'une fonction dont il est difficile de calculer l'inverse est spécifiée dans le standard ANSI X9.17.
Il est apparu que l'implémentation sur carte à puce d'un algorithme de chiffrement à clé secrète (par exemple l'algorithme DES) était vulnérable à des attaques consistant en une analyse différentielle de consommation de courant permettant de retrouver la clé secrète. Le principe de ces attaques DPA repose sur le fait que la consommation en courant du microprocesseur exécutant des instructions varie selon la donnée manipulée. Pour retrouver la clef secrète, il est nécessaire que le message d'entrée ou le message de sortie de l'algorithme de chiffrement soient connus.
Les deux procédés de génération de nombre aléatoire décrits dans la partie introductives de la demande sont donc vulnérables à des attaques de type attaques DPA puisque les nombres aléatoires renvoyés en sortie par ces deux procédés sont les messages de sortie de l'algorithme de chiffrement.
A partir de la consommation de courant de la carte à puce, il est donc possible de retrouver la clef K de chiffrement, et donc de prévoir ensuite la sortie du générateur aléatoire.

3. Le procédé de l'invention consiste en une modification des procédés de générations de nombre aléatoire décrits précédemment de façon à les rendre résistant contre des attaques de type DPA. Les deux procédés sont modifiés en ce qu'une variable entière intermédiare qui prendra la valeur du résultat de chiffrement de S avec l'algorithme DES utilisant la clé K est introduite dans la boucle de calcul juste après que S ait été remplacé pas S xor I.
Dans ce procédé amélioré de génération de nombres aléatoires, une attaque par mesure de courant de type DPA est impossible car les messages d'entrée et de

sortie de l'algorithme de chiffrement DES ne sont pas connus.

Concernant le point VIII
Observations relatives à la demande internationale

1. Seul des signes de référence au(x) dessin(s) sont à mettre entre parenthèses dans les revendications: le texte "pour Data Encryption Standard" ne doit pas être mis entre parenthèses (Article 6 PCT) puisqu'il défini l'acronyme DES.

2. Les termes "dont la qualité est jugée insufisante" et "de qualité jugée insufisante" de la revendication 2 sont vagues et équivoques, et laissent un doute quant à la signification des caractéristiques techniques auxquelles ils se réfèrent. L'objet de ladite revendication n'est donc pas clairement défini (article 6 PCT). Par ailleurs, aucune information concernant ce critère de qualité n'est définie dans la demande.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 08 mai 2001 (08.05.01)	
Demande internationale no PCT/FR00/02009	**Référence du dossier du déposant ou du mandataire** GEM 736
Date du dépôt international (jour/mois/année) 12 juillet 2000 (12.07.00)	**Date de priorité** (jour/mois/année) 15 juillet 1999 (15.07.99)
Déposant CORON, Jean-Sébastien etc	

1. L'office désigné est avisé de son élection qui a été faite:

   [X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

   13 février 2001 (13.02.01)

   [ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

   [ ] n'a pas été faite

   avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé
Maria Kirchner

no de téléphone: (41-22) 338.83.38